МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

SIBERIAN FEDERAL UNIVERSITY

660041, Россия, Красноярск, проспект Свободный, 79
телефон (391) 244-82-13, факс (391) 244-86-25
http://www.sfu-kras.ru e-mail: office@sfu-kras.ru

№

на № от

УТВЕРЖДАЮ

Ректор ФГАОУ ВО «Сибирский федеральный университет»,

Ваганов Евгений Александрович

«____» июня 2016г.

(Гербовая печать)

Отзыв

Ведущей организации о научно-практической ценности диссертации

Махорина Дмитрия Алексеевича

на тему «Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи», представленную на соискание ученой степени кандидата технических наук по специальности 05.11.07 – «Оптические и оптико-электронные приборы и комплексы» (технические науки)

Актуальность темы

Системы квантового распределения ключа (КРК), как известно, на сегодняшний день являются практически единственным примером успешной реализации технологий квантовых вычислений. Данная технология основана на понятии кубита – двухуровневой квантовой системы; в качестве наблюдаемых кубитов чаще всего используются квантовые состояния одиночных фотонов, закодированные в одном или нескольких неортогональных базисах. Защищенность от точного копирования (клонирования) таких состояний квантовых частиц основана на фундаментальном физическом ограничении, известном как теорема о запрете клонирования. Указанное ограничение не позволяет измерять состояния фотонов так, чтобы после измерения они всегда оставались в исходном квантовом состоянии. Отсюда следует, что любые попытки нелегитимного пользователя клонировать квантовые состояния фотонов в канале связи КРК неизбежно приведут к возмущению последних, т.е. к появлению ошибок на приемной стороне канала в формируемом системой первичном ключе. Изменение статистики результатов измерений уровня ошибок в первичном ключе на приемном конце и позволяет детектировать попытки клонирования состояний фотонов в квантовом канале. Указанная концепция, в отличие от широко распространенной сегодня схемы Хеллмана – Диффи, позволяет построить защищенную, т. е. обеспечивающую теоретически гарантированную секретность передачи ключей по технологии «одноразового блокнота» систему КРК. Многими экспертами такие системы рассматриваются

как критическая технология, способная обеспечить максимальную защиту систем коммуникаций, как на данный момент, так и в обозримом будущем.

Широкое внедрение технологии КРК в современное производство ограничивается рядом проблем, таких как задача разработки управляемых источников и устройств детектирования одиночных фотонов с высокой вероятностью в заданном квантовом состоянии при низком уровне ложных срабатываний, проблема увеличения дальности квантового канала системы и скорости генерации секретного ключа. Проведению исследований по поиску решения некоторых из указанных актуальных задач посвящена диссертационная работа Д.А.Махорина.

Структура и содержание работы

Диссертационная работа состоит из введения, четырех разделов, заключения и четырех приложений. Общий объем диссертации – 132 страницы, в том числе рисунков и схем – 63. Список использованной литературы содержит 111 наименований.

Во **введении** обоснована актуальность темы, определены цель и задачи исследований, представлены научная новизна и практическая значимость работы, изложены положения, выносимые на защиту.

В **первом разделе** рассмотрены основные принципы построения систем квантового распределения ключа. Изложен необходимый для создания формальной модели КРК формализм квантовой механики, в том числе описание состояний отдельных квантовых частиц, а также статистические характеристики ансамблей, представленных фотонами в чистых и смешанных когерентных и фоковских состояниях. Описаны эффекты интерференции амплитуд вероятности этих квантовых частиц, их регистрации и измерение с помощью ИМЦ. Рассмотрено понятие кудита (q-dit), как q-уровневое информационное состояние квантовой частицы, в т.ч. понятие кубита, реализуемое для $q = 2$.

Дано описание принципов формирования классических протоколов КРК на основе кубитов, приготовленных из одиночных фотонов с поляризационным, фазовым и временным кодированием.

Наиболее подробно рассмотрен предложенный Беннетом и Брассардом протокол BB84. Механизм защиты основан на случайной смене передающей стороной или пользователем А в каждом такте формируемой ею последовательности кубитов $\mathbf{m}_A$ состояний используемого для их приготовления вычислительного базиса. Возможность создания нелегитимным пользователем клон-машины для производства копий кубитов последовательности $\mathbf{m}_A$ при этом может быть связана лишь с несовершенством программно-аппаратного устройства системы КРК пользователя А и пользователя Б.

Второй раздел диссертации посвящен описанию аппаратной части системы КРК, а также модели ее функциональных характеристик. Дано обобщение модели Персоника помехоустойчивости систем волоконно-оптическими линиями связи на системы КРК с использованием в ПрОМ ЛФД в линейном режиме. Установлена связь схемотехнических решений на уровень ошибок P_f в квантовом канале, вносимых аппаратурой пользователя Б.

Для разработки модели трансформации time-bin кубитов было проведено обобщение известной модели симметричного ИМЦ на случай системы из не-

скольких последовательно включенных разбалансированных интерферометров. С этой целью в структурную схему ИМЦ, помимо вентилей Адамара H и фазовращательных вентилей P, вводится вентиль сдвига D, описывающий относительный временной сдвиг Δ в одном из плеч интерферометра. Показано, что за счет изменения разности фаз ϕ в плечах ИМЦ-А, Б, а также в волокнах квантового канала можно управлять структурой интерференционной картины в выходных портах ИМЦ-Б.

В **третьем разделе** диссертации изложены результаты разработки и исследования модели системы КРК, основанной на методе временного кодирования, предложенном С.Н. Молотковым (M04) и Debuisschert T., Boucher W. (DB04). Отмечается, что измерения состояний квантовых частиц в указанной схеме протокола КРК, фактически, являются проекционными, поскольку исключают неоднозначные оценки временного положения одиночного фотона в квантовом канале, а сам метод кодирования квантовых частиц является одноуровневым. Данная особенность организации КРК с временным кодированием снижает защищенность системы и требует дополнительных способов защиты протокола.

Показано, что одним из путей решения данной проблемы может являться использование подсистем статистического и интерферометрического контроля состояний принятых квантовых частиц. В работе предложены варианты возможной программно-аппаратной реализации указанных подсистем и результаты их симуляции.

Четвертый раздел посвящен разработке и исследованию оптоволоконной системы КРК, работающей по протоколу BB84 с временным кодированием квантовых частиц двухуровневыми динамическими состояниями – time-bin кубитов. Детально описаны логический и физический уровни реализации предложенного протокола BB84 с временным кодированием. Рассмотрены процессы приготовления и детектирования time-bin кубитов в системе из двух идентичных, разбалансированных ИМЦ. Показано, что в системах КРК с временным кодированием time-bin кубитов детектирование работы клон-машины нелегитимного пользователя может обеспечиваться за счет контроля распределения вероятностей регистрируемых квантовых частиц по тайм-слотам тактового интервала. В указанной системе также проводится контроль целостности передаваемых кубитов по средствам проверки наличия интерференции амплитуд вероятности. В предложенной схеме возможно использование информации о состояниях, не прошедших проверку базисов, для детектирования наличия нелегитимного пользователя. Такая информация обычно отбрасывается.

В **заключении** приводятся основные результаты работы.

Научная новизна диссертационной работы

Научная новизна результатов выполненной Махориным Д.А работы заключается в развитии математических и программных моделей для проектирования и оптимизации элементов и узлов системы КРК, в т.ч.:

1. Продемонстрирована эффективность использования time-bin кубитов для построения систем КРК.

2. Установлена зависимость порога срабатывания решающего устройства в ПрОМ системы КРК с вероятностью ложных символов и средней битовой скорости формирования системой первичного ключа.

3. Показано, что использование статистического и интерферометрического контроля одноуровневых состояний в системах КРК с временным кодированием по сравнению с известными аналогами позволяет усилить защищенность системы.

4. Разработан оригинальный способ построения системы КРК с временным кодированием time-bin кубитов, передаваемых по квантовому каналу связи.

5. Предложено использование данных о состоянии кубитов на выходе квантового канала связи, не прошедших процедуру согласования базисов в рамках протокола BB84 для детектирования перехвата данных

6. Предложен новый способ обнаружения атак на систему КРК, основанный на обработке временного статистического распределения сигналов на выходе ПрОМ по тайм-слотам в пределах тактового интервала.

Практическая значимость работы

Предложенные в диссертационной работе Махорина Д.А методики оценки помехоустойчивости систем КРК, моделей построения систем КРК с временным кодированием time-bin кубитов, подсистем интерферометрического и статистического контроля позволяют повысить надежность работы системы, скорость формирования секретного ключа, а также системную длину квантового канала. Указанные результаты представляют интерес для специалистов в области квантовой информатики и могут быть использованы в научных организациях, специализирующихся в области разработки систем защищенной связи нового поколения. Предложенная автором система квантового распределения ключей может использоваться для проведения НИР и ОКР в соответствующих организациях.

Степень достоверности результатов исследований

Достоверность полученных результатов диссертационного исследования обеспечивается применением современных апробированных методов научных исследований, обоснованностью предлагаемых моделей, решений и выводов, их адекватностью, соответствием ряда полученных данных результатам, установленным другими экспериментальными методами и опубликованным в научной литературе.

Замечания по диссертационной работе

1. В работе предлагается модель системы квантового распределения ключа с временным кодированием, которая базируется на протоколе BB84, при этом из диссертационной работы остаётся неясным, почему был выбран именно этот протокол, учитывая, что на данный момент известны и другие протоколы, построенные на его основе: BB84 с шестью состояниями, BB84(4+2) с четырьмя состояниями в двух базисах, и многие другие. В работе лишь даётся краткое упоминание о существовании протокола B92.

2. В работе предлагается использование статистического и интерферометрического контроля с целью выявления атаки типа «Человек посередине»

(Man in the middle, MITM). В части интерферометрического контроля предлагается использование имитовставки особых контрольных кубитов – «состояний ловушек», которая осуществляется неким случайным образом. При этом в работе не описано, каким именно способом обеспечивается генерация этих «случайных» контрольных кубитов.

3. Автор утверждает (стр. 91), что радикального увеличения скорости детектирования нелегитимного пользователя в оптическом канале связи с помощью интерферометрического контроля можно достичь при некой «протокольной организации», при этом описание протокола не приводит.

4. Автором получены количественные оценки времени детектирования нелегитимного пользователя предлагаемыми способами контроля одноуровневых состояний, однако в работе нет оценки ошибок первого и второго рода обнаружения, что, в свою очередь, ставит под сомнение оценку повышения защищённости системы с сохранением уровня стабильности её работы с точки зрения легитимных пользователей.

Сделанные замечания не влияют на общую положительную оценку диссертации Махорина Д.А.

Общая оценка диссертационной работы

Диссертационная работа Махорина Дмитрия Алексеевича «**Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи**» является завершенной научно-квалификационной работой на актуальную тему, обладающую научной новизной, в которой решена важная научно-техническая задача по совершенствованию систем квантового распределения ключей. По своей актуальности, научной новизне, объёму выполненных исследований и практической значимости полученных результатов представленная работа соответствует п.9 Положения о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г., предъявляемым к диссертациям на соискание учёной степени кандидата наук, а её автор, Махорин Дмитрий Алексеевич, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.11.07 – «Оптические и оптико-электронные приборы и комплексы». Полученные автором результаты являются новыми научными знаниями, и отвечает принятым критериям достоверности. Диссертация имеет все необходимые разделы от постановки задачи, обзора и методов решения задачи до результатов эксперимента, их анализа, выводов и заключения. Материалы работы представлены в 13 печатных работах, из которых восемь статей в журналах, входящих в перечень ВАК Минобрнауки РФ. В этих публикациях полностью отражено содержание диссертации.

Заключение

Считаем, что диссертационная работа Махорина Дмитрия Алексеевича «Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи», представленная на соискание ученой степени кандидата технических наук отвечает требованиям п. 9 «Положения о порядке присуждения ученых степеней» ВАК Минобразования и науки РФ. предъ-

являемым к кандидатским диссертациям, а ее автор, Махорин Дмитрий Алексеевич, заслуживает присуждения ему степени кандидата технических наук по специальности 05.11.07 – «Оптические и оптико-электронные приборы и комплексы».

Диссертационная работа и отзыв рассмотрены и одобрены на расширенном научном семинаре Института инженерной физики и радиоэлектроники (ИИФ и РЭ) и Института космических и информационных технологий (ИК и ИТ) ФГАОУ ВО «Сибирский федеральный университет».

Протокол № 1/5 от 06.05.2016.

Председатель семинара:
Зам. директора по научной
работе ИИФ и РЭ СФУ,
профессор, канд. техн. наук

Саломатов Юрий Петрович,
Телефон: +7(391) 291- 22- 78
Факс: +7(391) 291- 22- 78
E-mail: ysalomatov@sfu-kras.ru

Профессор кафедры «Фотоника и
лазерные технологии»
ИИФ и РЭ СФУ,
д-р физ.-мат. наук

Слабко Виталий Васильевич
Тел. +7(391) 249-74-22
Факс: +7(391) 249-74-22
E-mail: vslabko49@mail.ru